

Wireless Network Defense Proposers' Day Briefing

Dr. Wayne Phoel

April 1, 2013





BAA overview and schedule

- BAA 13-30 – Wireless Network Defense
 - Posted to www.fbo.gov on March 21, 2013
- Proposal Due Date: May 8, 2013
- Administrative, technical, or contractual questions should be sent via email to
 - DARPA-BAA-13-30@darpa.mil
- BAA-13-30 and associated amendments will be the official documents for this solicitation. They supersede statements made here.



Outline

- Reliability in Wireless Networks
- TA-1: Vulnerability Assessment
- TA-2: Information Reliability Estimation
- TA-3: Robust Network Control
- Anticipated Later Phases



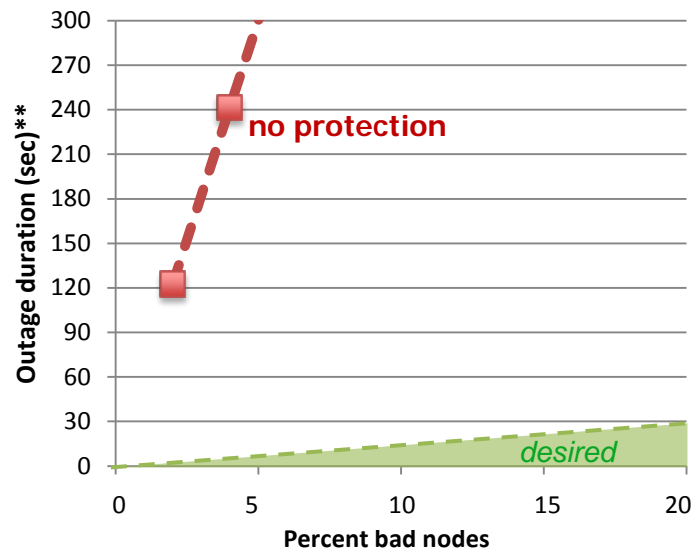
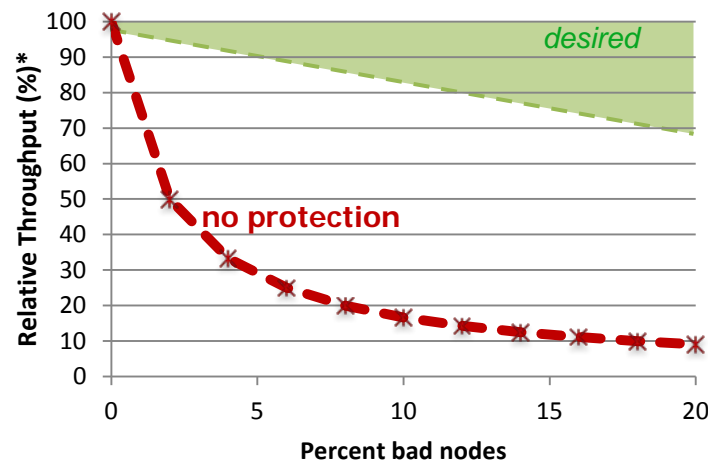
New approach needed to protect wireless networks

- Development of wireless networks has focused on efficiency over security
- Wireless networks are sensitive to control errors
 - Bad information in the network control can be debilitating: >2x loss throughput, >2-minute outages
- Compromise can have many causes
 - Captured radio, false radio, misconfiguration, unexpected corner case

We need to change how we control wireless networks

Compromise *will* happen

Effects of Misinformation*



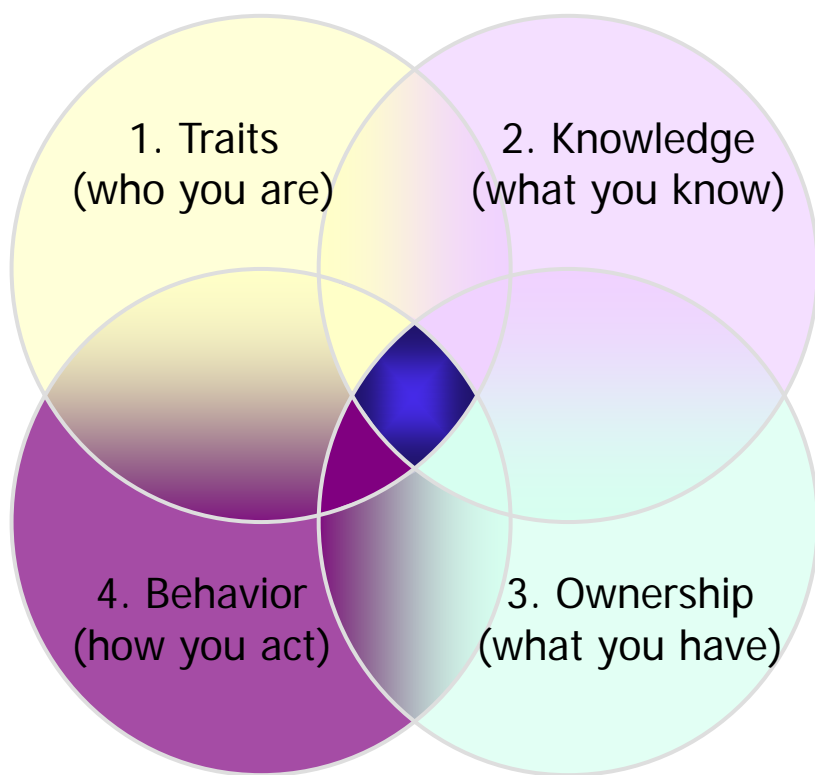
* Theoretical analysis of network control attack and protections

** 50 total nodes; simulation of attack on Ad hoc On-demand Distance Vector (AODV) routing protocol; non-collaborative attack



It's the network

For wireless devices, common security attributes don't distinguish good from bad
Behavior is the distinguishing characteristic

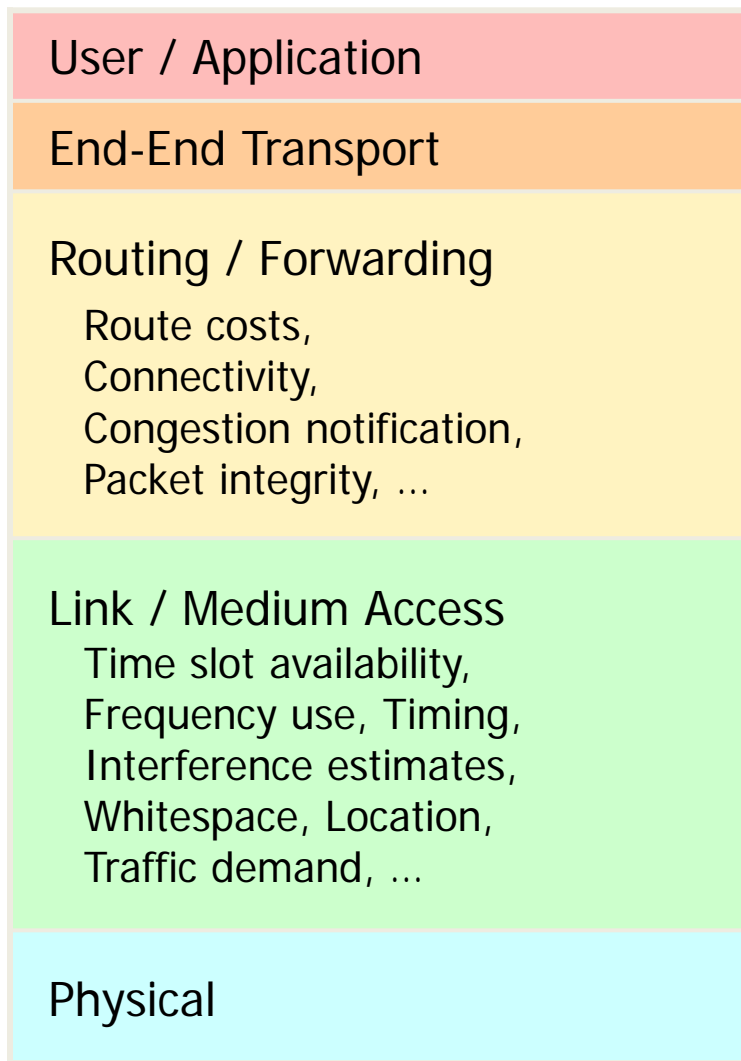


- Current security addresses individual radios
 - Just need one "impaired" radio to compromise the network
- Leverage rich and dynamic connectivity of wireless networks
 - Localized "neighborhood watch" to provide situational awareness
 - Robust network control implementation that acknowledges bad information is present

Develop a network-based solution for today's and future systems



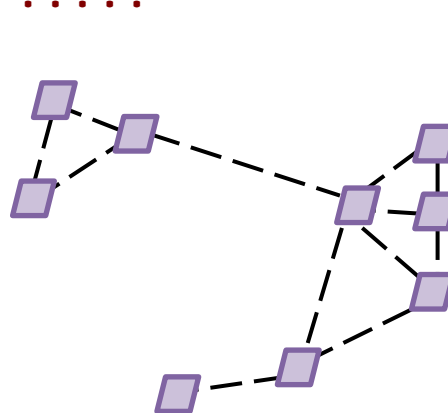
The soft spot in the network stack



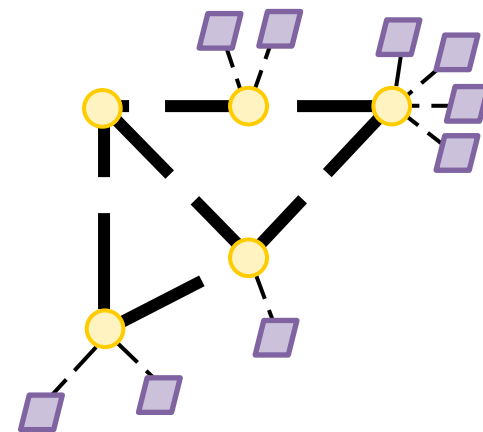
Cyber Defenses:

User authentication, Virus detection, Intrusion detection, Firewalls, Deep packet inspection, etc.

Wireless Network Defenses: ?????



Mobile Ad Hoc Networks



Mobile Hubs

Electronic Protections:

Spread spectrum, Transmission security (TRANSEC), Spatial discrimination, Interference cancellation, etc.

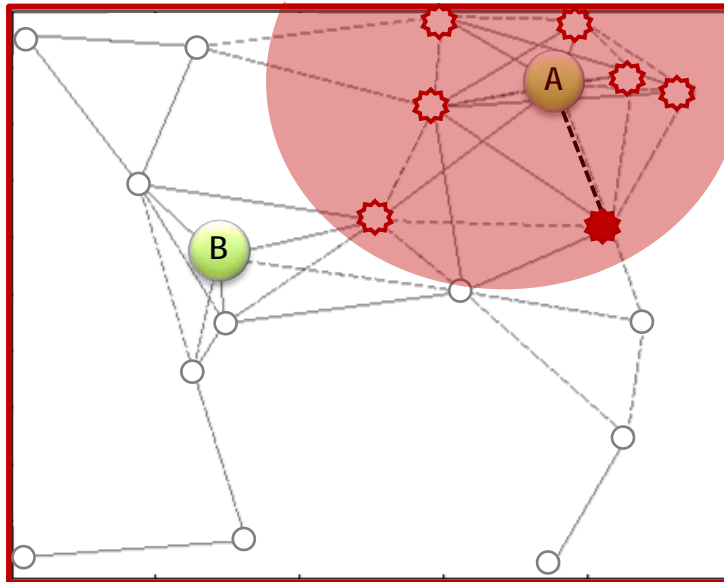
Routing example

Current: *unprotected network control*

Just **one of many** possible bad nodes can subvert **many** traffic flows

To get data from A to B...

What if a node misreports its ability to forward packets?



Example for illustrative purposes:

✱ = *Potential to disrupt flow from A to B*

★ = *Actual faulty / malicious node*

Any node closer than B to A can draw all traffic to it and it affects other neighbors similarly



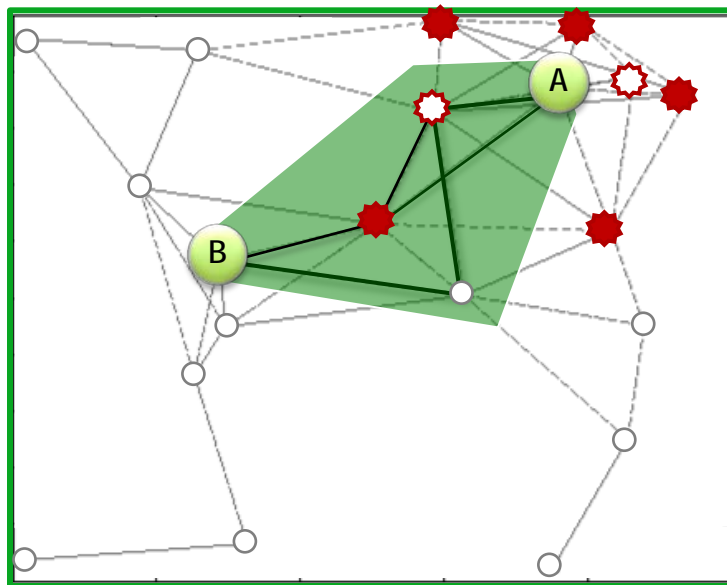
Protecting the network

Goal: *protected network control*


Many collaborating bad nodes needed for only **limited effect** on traffic

To get data from A to B...

What if nodes misreport their abilities to forward packets?



Example for illustrative purposes:

 = Potential to disrupt flow from A to B

 = Actual faulty / malicious node

Even with many compromised nodes surrounding A, the data finds its way out

Two new capabilities are needed:

1. Distinguish between reliable and unreliable nodes
2. Minimize effects of mischaracterization



Insights from economic and social networks

Economic / Social Networks	Wireless Networks	Challenges
Credit card fraud detection Sudden large purchases Unexpected locations Spending profiles	Step-change in statistics Number of neighbors, cost to destinations, etc. Cross-layer comparisons E.g., message completions and reported routes	1 Reliability Estimation
eBay buyer/seller ratings Based on ratings of raters	Share reliability estimates among neighbors	
Wikipedia editorial oversight Reputation-based access to tools and responsibilities	Scalability to affect network control based on proven reliability	2 Robust Control

Apply these concepts to efficient network-based protection of wireless

- Some expected behaviors based on first principles without needing large training set
- Reliability of *near* neighbors more important to decision-making



Wireless Network Defense program overview

- What it is not:
 - New radio program
 - New waveform development
- Near- and long-term goals
 - Create proven toolset to improve robustness of emerging wireless networks
 - Develop resilient foundation for future wireless systems
- Three phases
 - Technology development
 - System integration
 - Field test and transition
- Blue and red team thrusts



Phase 1 overview

- Primary goal to develop individual technology components and determine performance limits and trade-offs
 - Technical Area 1: Vulnerability Assessment
 - Technical Area 2: Reliability Estimation
 - Technical Area 3: Robust Control
 - Results will be used to define goals for Phase 2
- Secondary goal to encourage teaming for Phase 2 prototypes
- Encourage information sharing
 - Kickoff @ ~1 month
 - Technical Interchange Meetings @ 3 and 5 months
 - Technology Demonstrations @ 6 months 
 - Technical Interchange Meetings @ 9 and 11 months

Phase 2/3 BAA release
anticipated @ ~ month 7



TA-1: Vulnerability Assessment

Example Functions	
PLI, Video, Targeting, Chat, ...	
End-End ACK/NAK	Wireless Network Concerns
Security Association	Corrupt / discarded packets Incorrect route costs Incorrect neighbor counts
Packet Encryption	
Link State Routing	
Congestion Notification	
Packet Forwarding	
Dynamic Spectrum Access	Incorrect channel occupancy reports Incorrect slot availability reports Faulty time reports
Distributed Slot Allocation	
Time Alignment	
TRANSEC	
MIMO	

TA-1 to investigate broader threats to the control plane of wireless networks

Focus on those distinct from wired networks and needing novel solutions



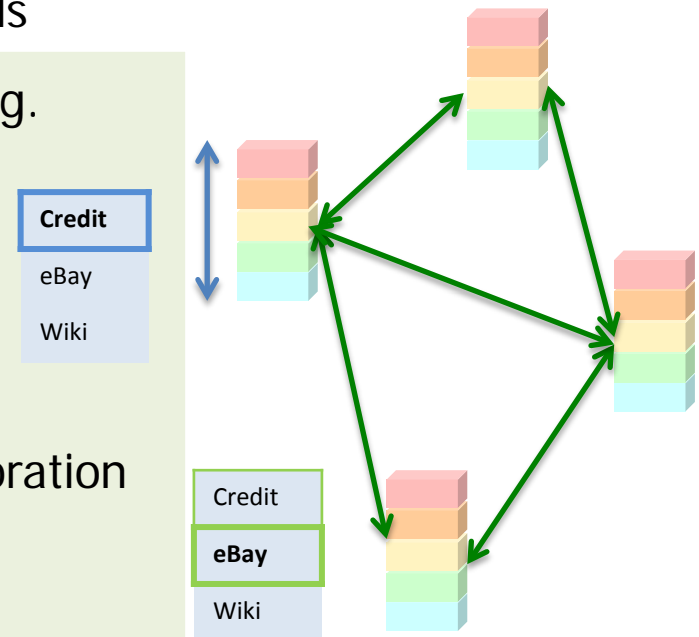
TA-1 Phase 1 details

- Initial vulnerability assessment and quantification to be based on Government-defined example system
 - Detailed example system and example scenarios to be provided prior to kickoff
- Throughout phase, assessment expands to include vulnerabilities to TA-2/3 proposed components and other system components deemed appropriate
- Responsibilities include
 - Define metric(s) to quantify network robustness
 - Assess candidate systems designs for weaknesses
 - Identify new threats / threat models
 - Define attack classes and implement select attacks to exercise TA-2/3 technologies
- Balance competing Red Team requirements
- Proposals to include costed options for red teaming in later phases



TA-2: Identification of reliable sources

- Resources are limited: capacity, power, ...
- Statistics not well characterized for parameters of concern
- Unified metric needed across disparate protocols
- Both passive and active approaches feasible, e.g.
- Determine indicators of bad information from statistics that are already shared
 - E.g., first principles to correlate message completion and advertised route costs
- Improve estimation through probes and collaboration
 - E.g., combining reliabilities from trusted neighbors



Determine indicators across network layers and in complex environments
Develop efficient multi-modal fusion for wireless network behavior



TA-2 Phase 1 details

- Goal is to characterize the performance limits and trade-offs of proposed reliability estimation approaches
 - How do we quantify reliability?
 - How do we fuse estimates across disparate protocols/parameters?
 - We do not want point solutions for specific protocols!
 - How accurately can we estimate reliability?
 - How does the accuracy change as network overhead is restricted?
 - How does the accuracy change as observability of attacks changes?
 - What new vulnerabilities are introduced?
- Government will not prescribe modeling tool to use
 - Performers should understand limitations of chosen tools
 - Government-defined scenarios to be provided prior to kickoff and during program
- Performers not required to divulge “secret sauce” at TIMs
 - Will need to present performance results with sufficient detail to enable understanding and trust of data



TA-3: Robust network control

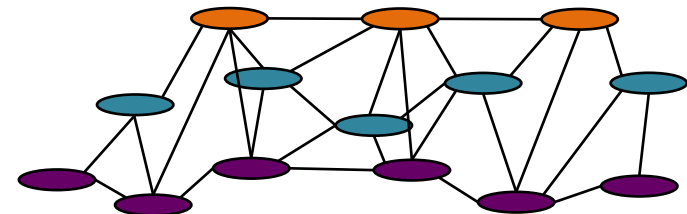
- Over-reacting can be as bad as doing nothing
- Network must function when bad information is missed and when good nodes seem bad
 - Develop understanding of how bad information propagates
 - Apply soft reliability estimates to network control calculations
 - Reputation-based decision authority

Example with three tiers: **Top tier makes control decisions**



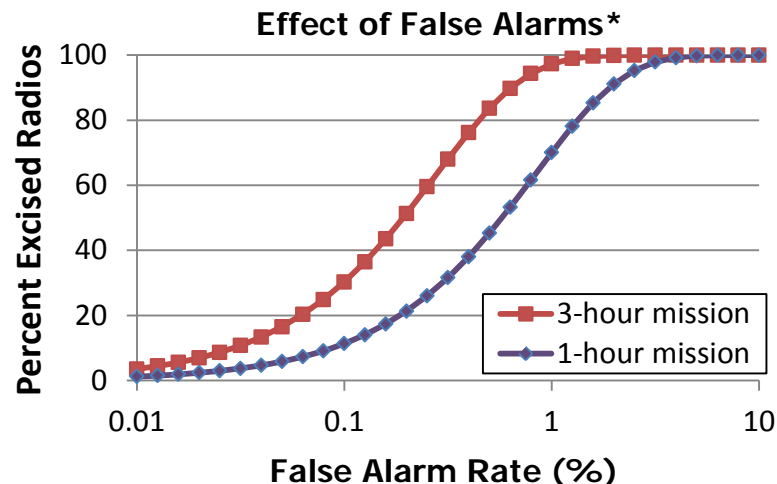
Second tier contributes statistics to control protocols

Lowest tier implements data plane functionality



- Enable reporting of most probable compromises for interrogation and mitigation

New network defenses must be more resilient than the system they're protecting



*Assumes 30-second detection period



TA-3 Phase 1 details

- Goal is to characterize the performance limits and trade-offs of proposed reliability estimation approaches
 - How do network control protocols change to accept reliability values?
 - How does network robustness change with control system topology?
 - Distributed with required agreement (e.g. Byzantine fault tolerance)
 - Tiered based on reliability values – and how do the logical connections enable / inhibit cascading of failures
 - Centralized control
 - How does network performance change as a function of attack severity, network overhead, and reliability estimation accuracy?
 - Should we implement completely new, robust protocols?
- Government will not prescribe modeling tool to use
 - Performers should understand limitations of chosen tools
 - Government-defined scenarios to be provided prior to kickoff and during program
- Performers not required to divulge “secret sauce” at TIMs
 - Will need to present performance results with sufficient detail to enable understanding and trust of data



Phases 2 and 3

- Blue Teams: system prototypes marry reliability estimation with robust control and demonstrate resilience to attack
- Red Team: investigate vulnerabilities specific to Blue Team designs
 - Requires access to Blue Team code/designs/algorithms/protocols
 - Design and implement attacks for tests
- Laboratory test near end of Phase 2
 - Potential for mix of real and emulated nodes (up to 100 total)
 - Emulated links among radios (leverage environment such as EMANE)
- Field test near end of Phase 3
 - Potential for mix of real and emulated nodes (~50)
 - Determine impact of real users and RF propagation on estimation algorithms and control protocols



BAA proposer categories

	Phase 1	Phase 2	Phase 3
TA-1	Current BAA Single performer Requires classified facility Cannot propose to TA-2 or TA-3	Current BAA Single performer Requires classified facility Cannot propose to TA-2/3	Current BAA Single performer Requires classified facility Cannot propose to TA-2/3
TA-2	Current BAA Multiple performers Does not require classified facility Cannot propose to TA-1 Can propose to TA-3	Future BAA Multiple (fewer) performers Requires classified facility	
TA-3	Current BAA Multiple performers Does not require classified facility Cannot propose to TA-1 Can propose to TA-2		



Evaluation criteria (descending order of importance)

1. Overall Scientific and Technical Merit

- The proposed technical approach is feasible, achievable, complete and supported by a proposed technical team that has the expertise and experience to accomplish the proposed tasks. Task descriptions and associated technical elements provided are complete and in a logical sequence with all proposed deliverables clearly defined such that a final product that achieves the goal can be expected as a result of award. The proposal clearly identifies major technical risks and clearly defines feasible planned mitigation strategies and efforts to address those risks. The proposal clearly explains the technical approach(es) that will be employed to meet or exceed each program goal and system metric listed in Section 1.2. and provides ample justification as to why the approach(es) is / are feasible. Other factors to be considered will include the structure, clarity, and responsiveness to the statement of work; the quality of proposed deliverables; and the linkage of the statement of work, technical approach(es), risk mitigation plans, costs, and deliverables of the prime contractor and all subcontractors through a logical, well structured, and traceable technical plan.

2. Potential Contribution and Relevance to the DARPA Mission

- The potential contributions of the proposed effort are relevant to the national technology base. Specifically, DARPA's mission is to maintain the technological superiority of the U.S. military and prevent technological surprise from harming our national security by sponsoring revolutionary, high-payoff research that bridges the gap between fundamental discoveries and their application. The Wireless Network Defense program has both near-term and long-term goals for affecting the national technology base: protect the many emerging wireless networks from advanced attacks, and develop a fundamentally robust foundation for the development of future wireless systems. Innovative and broadly applicable approaches are sought for each of these goals; point solutions to specific attacks will receive poor evaluations regarding their contribution and relevance to the DARPA mission.



Evaluation criteria, cont. (descending order of importance)

3. Proposer's Capabilities and/or Related Experience

- The proposer's prior experience in similar efforts must clearly demonstrate an ability to deliver products that meet the proposed technical performance within the proposed budget and schedule. The proposed team has the expertise to manage the cost and schedule. Similar efforts completed/ongoing by the proposer in this area are fully described including identification of other Government sponsors.

4. Realism of Proposed Schedule and Cost

- The proposer's abilities to aggressively pursue performance metrics in the shortest timeframe and to accurately account for that timeframe will be evaluated, as well as proposer's ability to understand, identify, and mitigate any potential risk in schedule. In addition, the proposed costs are realistic for the technical and management approach offered, as well as to determine the proposer's practical understanding of the effort. The proposal will be reviewed to determine if the costs proposed are based on realistic assumptions, reflect a sufficient understanding of the technical goals and objectives of the BAA, and are consistent with the proposer's technical approach (to include the proposed Statement of Work). At a minimum, this will involve review, at the prime and subcontract level, of the type and number of labor hours proposed per task as well as the types and kinds of materials, equipment and fabrication costs proposed. It is expected that the effort will leverage all available relevant prior research in order to obtain the maximum benefit from the available funding. For efforts with a likelihood of commercial application, appropriate direct cost sharing may be a positive factor in the evaluation. The evaluation criterion recognizes that undue emphasis on cost may motivate proposers to offer low-risk ideas with minimum uncertainty and to staff the effort with junior personnel in order to be in a more competitive posture. DARPA discourages such cost strategies.



Evaluation criteria, cont. (descending order of importance)

5. Plans and Capability to Accomplish Technology Transition

- The objective of this criterion is to establish that the capability and plans to transition or to expedite the transition of the technologies and products resulting from this program to the program(s) of record or to the operational military community is reasonable and achievable for the technology(ies) being developed. In addition, the evaluation will take into consideration the extent to which the proposed technical deliverables and intellectual property (IP) rights will potentially impact the Government's ability to transition technology



Summary

- The integrity of our wireless networks will be compromised
 - Due to misconfiguration or malicious attack
- We need to do something now to prevent significant loss
 - Develop toolset to apply to emerging wireless networks
 - Create new basis for development of robust networks
- Use the *network* to protect the *network*
 - Localized network situational awareness to quantify goodness of information sources
 - Network control mechanisms that account for information reliability
- Overarching goal is to maintain network performance for the users
 - Don't kill the network with overhead
 - Mitigate introduction of any new vulnerabilities



www.darpa.mil